JOURNAL OF NUMBER THEORY 12, 343–363 (1980)

Cyclic Isogenies and Nonstandard Arithmetic*

GERHARD FREY

Fachbereich Mathematik der Universität d.Saarlandes
D 6601 Saarbrücken, West Germany

Communicated by D. J. Lewis

Received July 9, 1979

For a prime N we denote by $X_0(N)(K)$ the set of K-rational points on the modul curve of elliptic curves with isogenies of degree N. We formulate arithmetical axioms for number fields K that imply finiteness properties of $X_0(N)(K)$. To prove the results we use the nonstandard version of the Siegel–Mahler theorem (A. Robinson and P. Roquette, *J. Number Theory* 7 (1975), 121–176) and the nonstandard interpretation of a sum formula derived from the local heights on elliptic curves.

INTRODUCTION

One of the most remarkable recent results in number theory is the complete description of all elliptic curves defined over $\mathbb{Q}$ with cyclic $\mathbb{Q}$-rational isogenies of prime degree due to Mazur in [2]. This description depends on the study of the mapping f of the Jacobian J_N of $X_0(N)$ onto the "Eisenstein quotient" $\tilde{J}$. The first important thing is that $\tilde{J}(\mathbb{Q})$ is finite cyclic of order $n =$ numerator $((N-1)/12)$ (cf. [1]), and the second fact is that in a neighborhood of (∞), f is given by a power series $\sum_{i=1}^{\infty} a_i q^i$ and the coefficients a_i are not too large. The first fact gives, by an easy geometric argument, that $|X_0(N)(\mathbb{Q})|$ is finite for $N \geqslant 11$; the second fact is used by Mazur to show that a curve with isogeny of prime degree $\geqslant 17$ defined over $\mathbb{Q}$ has to have potentially good reduction outside 2. The arguments involved in this proof are geometric, related to reduction theory and formal geometry. Then computations using the result of [4] concerning Galois representations induced by the points of order N of elliptic curves give the result.

So we have a very satisfying theory of isogenies of elliptic curves over $\mathbb{Q}$, and one would hope to extend Mazur's theory to arbitrary number fields K. In order to give ideas about the direction in which one could possibly advance we use the techniques of nonstandard extensions ${}^*K$ of K that are

* Part of this paper was written when the author was a visitor at Ohio State University, Columbus, Ohio. This visit was partly supported by the Deutsche Forschungsgemeinschaft.

0022-314X/80/030343–21$02.00/0

described in [3]. By these methods we can transform a considerable part of the geometric considerations into arithmetic arguments and the infinite places play an important role, as it is typical for this theory. (Another typical effect is that we get less exact quantitive results: The nonstandard methods always prove only the finiteness of a set.)

Using the nonstandard version of the finiteness theorem of Siegel and Mahler given in [3] we get that the finiteness of $X_0(K)$ is equivalent to an arithmetic axiom, Axiom A_N, which claims that the reduction types of cyclic isogenies defined over K in places with bad reduction are determined by the type in one special place with bad reduction. The proof of this fact is rather formal; in order to understand the meaning of Axiom A_N and of a more general Axiom B in a better way we look at a sum formula (that itself seems to be of some interest) for local heights related to isogenies (Section 3). We get this formula in a completely "standard way" for isogenies over K but the most striking interpretation of this formula is given in the nonstandard interpretation (formula (11a)), where the differences between finite and infinite primes in $^*K$ almost vanish. The sum formula imposes strong conditions on the denominator of the j-invariant of an elliptic curve with cyclic isogeny; using the formula we can show that the number of K-rational cyclic isogenies of an elliptic curve whose invariant has a bounded denominator is bounded if K is totally real (Corollary 4.4), and if $K = \mathbb{Q}$ we get that there are (up to $\mathbb{C}$-isomorphisms) only finitely many such curves with a cyclic $\mathbb{Q}$-rational isogeny (cf. Proposition 4.5 and part of the proof of Proposition 5.3). The fact that the denominator of j is bounded makes it easy to use the formula, and now one sees that Axioms A_N (resp. B) do exactly the same, and hence if K is a field satisfying Axiom B we get corresponding results for curves with nonintegral j-invariants.

If we take $K = \mathbb{Q}$ to test our results we see that Axiom B is a consequence of the fact that $\tilde{J}(\mathbb{Q})$ is finite of order n, and using the description of f:

$$J_N \to \tilde{J} \text{ interpreted over } {}^*\mathbb{C} \text{ (for nonstandard } N)$$

we finally get that there are only finitely many curves with $\mathbb{Q}$-rational cyclic isogenies of prime degree $\geqslant 11$. (Of course the necessary input of results due to Mazur is so great that this is no "new and simple proof," all that we did was replace some arguments of the reduction theory and of the formal geometry by the consideration of the sum formula and the infinite prime.)

To conclude we want to emphasize that the use of nonstandard methods gives no magic tool to solve mathematical problems; in our case we translated the finiteness condition for $X(N)(K)$ into (standard) arithmetic properties of elliptic curves with K-rational cyclic isogenies (which we can only verify in the "well-known" case $K = \mathbb{Q}$) and we found a sum formula for the j-invariant of such curves whose nonstandard interpretation over $^*K$ seems to be interesting enough to justify further investigations.

1. Notations and Definitions

1. In the following we fix a finite algebraic number field K over $\mathbb{Q}$, and M_K are the places of K, $\{v_1,..., v_t\} = M_{K,\infty}$ the infinite places, and M'_K the finite places. By $|\ |_j$ we denote the absolute value corresponding to v_j $(j = 1,..., t)$ and normed in the following way: if σ_j is an embedding of K in $\mathbb{C}$ related with v_j then for $x \in K$ we have:

$$\begin{aligned} |x|_j &= |\sigma_j(x)| \qquad \text{if} \quad \sigma_j \text{ is a real embedding} \\ &= |\sigma_j(x)|^2 \qquad \text{if} \quad \sigma_j \text{ is not real.} \end{aligned}$$

For $\mathfrak{p} \in M'_K$ let $v_\mathfrak{p}$ be the valuation in $\mathfrak{p}$ with value group $\mathbb{Z}$, and $N(\mathfrak{p}) =$ Norm of $\mathfrak{p}$. Then for all $x \in K^*$ we have the relation

$$\sum_{j=1}^{t} \log |x|_j = \sum_{\mathfrak{p} \in M'_K} v_\mathfrak{p}(x)\, N(\mathfrak{p}).$$

With $K_\mathfrak{p}$ resp. $K(\mathfrak{p})$ we denote the completion of K resp. the residue field with respect to $\mathfrak{p} \in M'_K$. If L is an extension field of K then $\bar{L}$ is the algebraic closure of L.

Let $^*K$ be a nonstandard extension of K as it is defined in [3]. If A is a mathematical structure defined over K then $^*A$ denotes the corresponding object that is defined over $^*K$.

Examples. $^*K$ is an algebraic field extension of $^*\mathbb{Q}$ of degree $[K:\mathbb{Q}]$. A place $\mathfrak{p} \in M_K$ extends uniquely to a place of $^*K$ which we denote by the same symbol. The set of all these extensions form the subset of standard primes of $^*M_K$, where $^*M_K$ denotes the set of all internal places of $^*K$ (as extension of K). The set of archimedean places in $^*M_K$ is equal to $v_1,..., v_t$. The value groups of valuations belonging to $\mathfrak{p} \in {}^*M_K$ are contained in $^*\mathbb{R}$. If we define $v_\mathfrak{p}$ and $N(\mathfrak{p})$ $(\mathfrak{p} \in {}^*M_K)$ analogously to the above we get again: For all $x \in {}^*K$ we have

$$\sum_{j=1}^{t} \log |x|_j = \sum_{\mathfrak{p} \in {}^*M'_K} v_\mathfrak{p}(x) \cdot N(\mathfrak{p}).$$

Now $^*\mathbb{R}$ contains $\mathbb{R}$ in a natural way, but $^*\mathbb{R}$ has infinitely large numbers and infinitesimals.

Definition. If $x, y \in {}^*\mathbb{R}$ then

$x \approx y$ if $x - y$ is infinitesimal,

$x \doteq y$ if $|x - y|$ finite,

$x \gg y$ if $x - y$ is infinitely large.

Let $K[X]$ be the ring of polynomials over K. Then ${}^*K[X] = \{\sum_{i=0}^{N} a_i X^i;$ $N \in {}^*\mathbb{N}$, $a_i \in {}^*K\}$, and ${}^*K(X) = \mathrm{Quot}({}^*K[X])$. The analogous constructions can be done with several indeterminates. If we have chosen a fixed embedding of K in $\mathbb{C}$ this induces an embedding of ${}^*K \subset {}^*\mathbb{C}$, and we have ${}^*\bar{K} = \{x \in {}^*\mathbb{C}, \exists f(X) \in {}^*K[X]$ with $f(x) = 0\} \supsetneq \overline{({}^*K)}$.

The most important principle we will use in order to prove theorems about K by using ${}^*K$ is the following: If S is an internal set of objects defined over ${}^*K$ and if S contains only standard objects, then S is finite. (For the definition of "internal" as well as for a detailed exposition of the nonstandard techniques see [3], a reference that we will use throughout the following without citing it.)

2. Let E be an elliptic curve defined over K. E is determined (up to isomorphisms) by the absolute invariant j and the Hasse-invariant δ. We find an equation for E of the following type:

$$y^2 = x^3 - g_2 x - g_3 \qquad \text{with} \quad g_i \in K,$$

$$\Delta = 4g_2^3 - 27g_3^2 \neq 0 \qquad \text{and} \qquad j = 12^3 \cdot 4 \cdot g_2^3 \cdot \Delta^{-1},$$

$$\delta \equiv -\tfrac{1}{2} g_2 \cdot g_3 \bmod (K^*)^2 \qquad (\text{if } j \neq 0,\ 12^3).$$

For any overfield L of K the L-rational points of E (together with the infinite point (∞, ∞) as zero-element) form an abelian group, the addition is defined by rational functions with coefficients in $\mathbb{Z}[g_2, g_3]$. If $n \in \mathbb{N}$ is given then the multiplication by n induces a homomorphism on $E(\bar{K})$, and the kernel E_n of this homomorphism has order n^2. A point $P = (x, y)$ is in E_n iff $P = (\infty, \infty)$ or x is a zero of a polynomial $\psi_n(x) \in \mathbb{Z}[g_2, g_3, x]$ (of degree $(n^2 - 1)/2$ if n is odd).

Let E_1, E_2 be two elliptic curves defined over K. Let Q_1, Q_2 be elements in $K(x, y)$ such that for all $(x_1, y_1) \in E_1(\bar{K})$ we have $(Q_1(x_1, y_1), Q_2(x_1, y_1)) \in E_2(\bar{K})$ and the mapping η given by $(x_1, x_2) \to (Q_1(x_1, y_1), Q_2(x_1, y_1))$ is compatible with $+$ (on E_1 resp. E_2) and the kernel of η is finite. Then η is a K-rational isogeny from E_1 to E_2 of degree $\eta := |\mathrm{Kernel}(\eta)|$. There is an isogeny $w(\eta)$ from E_2 to E_1 that is K-rational too, and $w(\eta) \circ \eta = \deg(\eta) \cdot \mathrm{id}_{E_1}$.

Now assume that $\deg(\eta) = N \in \mathbb{P}$, where $\mathbb{P}$ is the set of primes in $\mathbb{N}$. Then there is exactly one subgroup of $E_1(\bar{K})_N$ generated by an element $P \in E(\bar{K})_N$ of order N such that $\mathrm{kernel}(\eta) = \langle P \rangle$ and $E_2 \cong E_1/\langle P \rangle$. $\langle P \rangle$ is mapped into itself by all automorphisms of $\mathbb{C}|K$. We say: η is a cyclic K-rational isogeny of degree N.

E_2 is (up to K-isomorphy) uniquely determined by the pair $(E_1, \langle P \rangle)$.

If j_i are the absolute invariants of E_i then (j_1, j_2) is a zero of the "invariant polynomial" $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$. $X_0(N)$ is defined as the

nonsingular projective curve corresponding to the equation $\Phi_N(X, Y) = 0$. Then there are two "cusps" (0) and (∞) lying in $X_0(N)(K)$ such that the points $x \in X_0(N)(K)\backslash\{(0), (\infty)\}$ correspond to K-rational isogenies of degree N of elliptic curves (up to $\bar{K}$-isomorphisms). If $N \geqslant 23$ then the genus of $X_0(N)$ is larger than 1. The following proposition is well known (and easily proved by using the theory of Tate curves):

PROPOSITION 1.1. *Let $N \in \mathbb{P}$ and $\mathfrak{P}$ be the place of $K(X)$ with $v_{\mathfrak{P}}(X) = -1$, $v_{\mathfrak{P}}(K^*) = 0$. Let X_N be a zero (in $\overline{K(X)}$) of $\Phi_N(X, Y)$. Then there are extensions $\mathfrak{Q}_1$ and $\mathfrak{Q}_2$ of $\mathfrak{P}$ to $K(X, X_N)$ such that $v_{\mathfrak{Q}_1}(X/X_N) > 0$ and $v_{\mathfrak{Q}_2}(X/X_N) < 0$.*

3. From the formulation of the well-known facts in **2** one sees immediately that one can define (for elliptic curves E defined over $^*K$):

(i) Multiplication with $n \in {}^*\mathbb{N}$: This is a homomorphism of $E(^*\bar{K})$ onto $E(^*\bar{K})$ described by elements $P_n, Q_n \in {}^*(K(X, Y))$.

(ii) The kernel of this homomorphism $E(^*\bar{K})_n$ is isomorphic to ${}^*\mathbb{Z}/n \times {}^*\mathbb{Z}/n$, and the X-coordinates of the points of order n are the zeros of a "$*$-polynomial" $\psi_n \in {}^*(\mathbb{Z}[g_2, g_3, X])$.

(iii) Instead of isogenies we define "$*$-isogenies" η given by functions in ${}^*(K(X, Y))$. The kernel of η is $*$-finite, and $\deg(\eta) = |\ker(\eta)| \in {}^*\mathbb{N}$.

(iv) If $\deg(\eta) = N \in {}^*\mathbb{P}$ is a prime, then $\ker(\eta) = \langle P \rangle$, with $P \in E(^*\bar{K})_N$ and $\langle P \rangle$ is invariant under all automorphisms of ${}^*\mathbb{C}\,|\,{}^*K$.

2. A CONDITION FOR THE FINITENESS OF $|X_0(N)(K)|$

In this paragraph N is a fixed prime in $\mathbb{P}$, $N \geqslant 23$, and $M_N \in \mathbb{N}$.

DEFINITION. K satisfies Axiom A_N with bound M_N if for all isogenies η: $E \to E_N$ of degree N and defined over K we have: If there is a $\mathfrak{p}_0 \in M_K'$ with $N(\mathfrak{p}_0) \geqslant M_N$, $v_{\mathfrak{p}_0}(j(E)) < 0$ and $v_{\mathfrak{p}_0}(j(E)/j(E_N)) < 0$ then for all $\mathfrak{p} \in M_K'$ with $N(\mathfrak{p}) \geqslant M_N$ and $v_{\mathfrak{p}}(j(E)) < 0$ we have $v_{\mathfrak{p}}(j(E)/j(E_N)) < 0$.

Axiom A_N (with bound M_N) has an obvious interpretation in $^*K$, and K satisfies A_N if and only if $^*K$ satisfies A_N.

PROPOSITION 2.1. *The following two statements are equivalent:*

(i) *There is an M_N such that K satisfies A_N with bound M_N.*

(ii) *$X_0(N)(K)$ is a finite set.*

Proof. That (ii) implies (i) is obvious, for there are only finitely many j-

invariants we have to look at, and these invariants have only finitely many places in the denominator.

(i) $\Rightarrow$ (ii): Assume that $|X_0(N)(K)| = \infty$. Then there is a point (j, j_N) in $X_0(N)(^*K)\backslash X_0(N)(K)$. K is algebraically closed in $^*K$, and hence j is transcendental over K, and $K(j, j_N)$ is the function field of $X_0(N)$ over K.

Let $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ be extensions of the place $\mathfrak{P} \leftrightarrow 1/j$ of $K(j)$ to $K(j, j_N)$ such that $v_{\mathfrak{Q}_1}(j/j_N) > 0$ and $v_{\mathfrak{Q}_2}(j/j_N) < 0$. $\mathfrak{Q}_1$ and $\mathfrak{Q}_2$ exist (Proposition 1.1). Now the nonstandard version of the theorem of Siegel–Mahler given in [3] implies the existence of places $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in $^*M'_K\backslash M'_K$ with $\mathfrak{p}_1|K(j, j_N) = \mathfrak{Q}_1$ and $\mathfrak{p}_2|K(j, j_N) = \mathfrak{Q}_2$. Hence:

$$v_{\mathfrak{p}_1}(j) < 0 \text{ and } v_{\mathfrak{p}_1}\left(\frac{j}{j_N}\right) > 0, \qquad v_{\mathfrak{p}_2}(j) < 0 \text{ and } v_{\mathfrak{p}_2}\left(\frac{j}{j_N}\right) < 0.$$

But $\mathfrak{p}_i$ is a nonstandard place, and so $N(\mathfrak{p}_i) \gg 0$ for $i = 1, 2$. Especially $N(\mathfrak{p}_i) > M_N$, and we get a contradiction to axiom A_N.

How can one verify Axiom A_N (which should be valid for all number fields if Mordell's conjecture is true for the curves $X_0(N)$)? One possibility is the following: Let J_N be the Néron minimal model of the Jacobian of $X_0(N)$ over $\mathbb{Z}$, and let $A/\mathbb{Z}$ be a quotient of J_N, such that the images of the cusps (0) and (∞) are different. Assume $|A(K)| < \infty$. Then it is easy to see that Axiom A_N is satisfied by K.[1]

In this case even more is true: K satisfies

AXIOM B. *There is a natural number M only depending on* $\deg[K:\mathbb{Q}]$ *such that for all primes $N > M$ the following is true: If $\eta: E \to E_N$ is a K-rational isogeny of degree N and if j and j_N are the absolute invariants of E and E_N and if there is a $\mathfrak{p}_0 \in M'_K$ with $v_{\mathfrak{p}_0}(j) < 0$ and $v_{\mathfrak{p}}(j/j_N) < 0$ then we have for all $\mathfrak{p} \in M'_K$ with $v_{\mathfrak{p}}(j) < 0$: $v_{\mathfrak{p}}(j/j_N) < 0$.*

Of course Axiom B has an interpretation in $^*K$ (with the same M), and so we have for $N \in {}^*\mathbb{P}\backslash\mathbb{P}$: Either $v_{\mathfrak{p}}(j/j_N) < 0$ for all $\mathfrak{p} \in {}^*M'_K$ with $v_{\mathfrak{p}}(j) < 0$ or $v_{\mathfrak{p}}(j/j_N) > 0$ for all such $\mathfrak{p}$.

It is clear that Axiom B is true if there are only finitely many elliptic curves (up to $\bar{K}$-isomorphisms) defined over K that have a K-rational isogeny of prime degree. In Section 5 we will try to see how far we can go in the converse direction.

One main result in [1, 2] is that the Eisenstein quotient $\tilde{J}$ of J_N has the right properties for $K = \mathbb{Q}$: $J(\mathbb{Q}) = \langle \tilde{c} \rangle$ and $\operatorname{ord}(\tilde{c}) =$ numerator of $(N-1)/12 = \operatorname{ord}((0) - (\infty))$ for $N \geqslant 13$. Hence Axiom B is valid for $\mathbb{Q}$. In [2] Mazur describes the behaviour of the mapping on $f: J_N \to \tilde{J}$ in a neighborhood of (∞). This will be important in Section 5.

[1] If $|A(K)| < \infty$ then of course purely geometric arguments show that $X_0(N)(K)$ is finite, too.

Now assume that we do not know if Axiom A_N or B is true for a number field $L \supset K$. In this case we can prove "relative" statements.

DEFINITION. An elliptic curve E defined over L is "balanced" (relative to K) if (for $\mathfrak{p} \in M_L'$) $v_{\mathfrak{p}}(j(E)) < 0$ implies $v_{\mathfrak{p}'}(j(E)) < 0$ for all $\mathfrak{p}' \in M_L'$ with $\mathfrak{p}'|K = \mathfrak{p}|K$.

(Especially all curves defined over K are balanced, and if E is isogeneous to E' and E is balanced, then E' is balanced, too.)

Let $\eta_N : E \to E_N$ be an L-rational isogeny of degree N between balanced curves with corresponding point $x = (j, j_N)$ in $X_0(N)(L)$. Let $\mathfrak{p}$ be in M_L' with $v_{\mathfrak{p}}(j) < 0$. Then the order of x mod $\mathfrak{p}$ in $J_N(L(\mathfrak{p}))$ is either 0 if $v_{\mathfrak{p}}(j/j_N) < 0$ or $n =$ numerator of $((N-1)/12) > 0$.

In the second case x is congruent to c mod $\mathfrak{p}$. Now apply the norm map of the extension L/K to x. Then $N_{L/K}(x) \in J_N(K)$ and the facts that the cusps of $X_0(N)$ are $\mathbb{Z}$-rational and that E is balanced imply: If $n > \deg(L:K)$ and if there is a $\mathfrak{p} \in M_L'$ with $v_{\mathfrak{p}}(j) < 0$ and $x \not\equiv (0) \bmod \mathfrak{p}$ then we have for $\mathfrak{P} = \mathfrak{p}|K$: $N_{L/K}(x) \not\equiv (0) \bmod \mathfrak{P}$.

We formulate a stronger version of Axiom A_N for K:

AXIOM A_N'. *There is a number M (depending on $[K:\mathbb{Q}]$) such that for all $y \in J_N(K)$ the following is true: If (for $\mathfrak{P}_0 \in M_K'$) $N(\mathfrak{P}_0) > M$ and $y \equiv (0)$ mod $\mathfrak{P}_0$ then we have for all $\mathfrak{P} \in M_K'$ with $N(\mathfrak{P}) > M$ and $y \equiv c^{\lambda}\mathfrak{P}$ mod $\mathfrak{P}$: $y \equiv (0)$ mod $\mathfrak{P}$.*

(If $K = \mathbb{Q}$ then Axiom A_N' is true for $N \geqslant 13$.)

If K satisfies Axiom A_N' then L satisfies Axiom A_N restricted to balanced curves for $n > [L:K]$, and so we get

PROPOSITION 2.2. *Assume that Axiom A_N' is valid in K. Then for all extension fields L of K with $[L:K] < n$ the set of $\mathbb{C}$-isomorphy classes of balanced elliptic curves defined over L with L-rational isogeny of degree N is finite.*

Proposition 2.1 shows the importance of (the arithmetic) axiom A_N for the finiteness of $X_0(N)(K)$ for a fixed prime N. One would hope that Axiom B should give some information for all N. But if one wants to use the nonstandard technique that gave the proof of the proposition one sees that $*$-isogenies have to be considered, and so we have to describe $X_0(N)(*K)$ for $N \in {}^*\mathbb{P}\backslash\mathbb{P}$. But the theorem of Siegel and Mahler does not apply to these objects ("$*$-curve"), and hence we have to look for other global relations satisfied by points in $X_0(N)(*K)$. One relation of this type is given by the local heights that we will study in the next section.

3. Local Heights on $X_0(N)$

1. Following [5] the local height functions are derived from Néron's "quasifunctions": Let x be a point in $X_0(N)(K)\backslash\{(0),(\infty)\}$ with $N\in\mathbb{P}$, $N\neq 2$, and $\eta\colon E\to E_N$ a corresponding K-rational isogeny with kernel $\langle P\rangle$. Let j be the invariant of E.

If $K_1=K(P)$ then K_1 is a Galois extension of K with a cyclic Galois group whose order divides $N-1$. Let v be a valuation of K and $v_1,\dots,v_t$ all extensions of v to K_1 with $v_i|K=e\cdot f\cdot v$, where e is the ramification index and f the residue field degree of v in K_1. Let δ_{v_i} be the quasifunction on $E\times K_1$ as defined in [5]. (We will give the explicit expressions for δ_{v_i} below.)

DEFINITION.

$$\delta_v(x):=\sum_{j=1}^{t}\sum_{i=1}^{N-1}\delta_{v_j}(iP).$$

If σ is an element in $G(K_1|K)$ then the definition of δ_{v_i} implies

$$\delta_{\sigma^{-1}v_j}(iP)=\delta_{v_j}(\sigma(iP)),$$

and hence

$$\begin{aligned}\delta_v(x)&=\sum_{i=1}^{N-1}\sum_{\sigma\in G(K_1|K)/G(v)}\delta_{v_1}(i\sigma P)=t\cdot\sum_{i=1}^{N-1}\delta_{v_1}(iP)\\&=[K_1:K]\sum_{i=1}^{N-1}\delta_w(iP),\end{aligned}$$

where $G(v)$ is the inertia group of v and w is any extension of v to K_1 with $w|K=v$.

Now we have a product formula in K if we norm v (and hence w) in a suitable way, and since P is a torsion point this implies that

$$\sum_{v\in M_K}\delta_v(x)=0,$$

or (1)

$$\sum_{w|v\in M_K}\sum_{i=1}^{N-1}\delta_w(iP)=0,$$

In order to exploit this formula we have to compute $\delta_v(x)$ in several cases.

First assume that v is a nonarchimedean valuation with $v(j)\geqslant 0$. Then E

has potential good reduction in v, and in order to compute $\delta_w(iP)$ we can assume that E has good reduction in w (cf. [5]), and hence

$$\begin{aligned}\delta_w(iP) &= 0 && \text{if} \quad w \nmid N \\ &= \frac{c_v}{N-1} \cdot \log N(v) && \text{if} \quad w \mid N\end{aligned}$$

with $c_v \in \{-1, -\frac{1}{2}, -\frac{1}{3}\}$.

This gives us

$$\sum_{\substack{v \in M_K' \\ v(j) \geqslant 0}} \delta_v(x) = \sum_{\substack{v \mid N \\ v(j) \geqslant 0}} c_v \log N(v) = c_N' \cdot \log N \tag{2}$$

where $|c_N'| \leqslant [K:\mathbb{Q}]$ and the denominator of c_N' divides 6.

Next assume that $v(j) < 0$. We can assume that $E \times K_{1,w}$ is a Tate curve, and so our point P corresponds to an element $\zeta^{\mu_1} \cdot q^{\mu_2/N}$ in $K_{1,w}$, where ζ is an Nth root of unity and q is the period of $E \times K_w$ ($w(q) = -v(j)$). We can choose (μ_1, μ_2) with $0 \leqslant \mu_i \leqslant N-1$, and (μ_1, μ_2) is not equal to $(0, 0)$.

The first case we look at is that $\mu_2 \neq 0$. This means: $x \equiv (0) \bmod v$. Then formula B35 in [5] implies:

$$\sum_{i=1}^{N-1} \delta_w(iP) = \sum_{i=1}^{N-1} \frac{6i/N - 6i^2/N^2 - 1}{12} v(j) = \frac{N-1}{12N} v(j).$$

Using the normed valuation $v_\mathfrak{p}$ we get: If $\mathfrak{p} \in M_K'$, $v_\mathfrak{p}(j) < 0$ and $x \equiv (0) \bmod \mathfrak{p}$ then

$$\delta_v(x) = \frac{N-1}{12N} v_\mathfrak{p}(j) \cdot \log N(\mathfrak{p}). \tag{3}$$

If $x \equiv (\infty) \bmod \mathfrak{p}$ then again formula B35 in [5] gives

$$\delta_v(x) = -\frac{N-1}{12} v_\mathfrak{p}(j) \log N(\mathfrak{p}) + \varepsilon_\mathfrak{p} \log N(\mathfrak{p}) \tag{4}$$

with

$$\begin{aligned}\varepsilon_\mathfrak{p} &= 1 && \text{if} \quad \mathfrak{p} \mid N \\ &= 0 && \text{if} \quad \mathfrak{p} \nmid N.\end{aligned}$$

Putting (2), (3) and (4) together we get

$$12 \sum_{v \in M_K'} \delta_v(x) = \sum_{\substack{\mathfrak{p} \in M_K' \\ v_\mathfrak{p}(j) < 0 \\ x \equiv (\infty) \bmod \mathfrak{p}}} (1-N) v_\mathfrak{p}(j) \log N(\mathfrak{p}) + \sum_{\substack{\mathfrak{p} \in M_K' \\ v_\mathfrak{p}(j) < 0 \\ x \equiv (0) \bmod \mathfrak{p}}} \frac{N-1}{N} v_\mathfrak{p}(j) \log N(\mathfrak{p}) + \varepsilon_N'' \tag{5}$$

with $\varepsilon_N'' = c_N'' \cdot \log N$, $c_N'' \in \mathbb{Z}$ and $|c_N''| \leqslant 24[K:\mathbb{Q}]$.

Now we have to compute the local height of x in the archimedean places too. So let v_l be an archimedean place. Assume that $K_{v_l} = \mathbb{C}$ (without loss of generality). Since δ_{v_l} is a function on the $\mathbb{C}$-isomorphy classes of E we can assume that there is a $\tau_l \in \mathbb{C}$ with $\operatorname{Im}(\tau_l) > 0$, $|\operatorname{Re}(\tau_l)| \leqslant \frac{1}{2}$ and $|\tau_l|_l \geqslant 1$ such that $E \times \mathbb{C} = \mathbb{C}/(\mathbb{Z} + \tau_l \mathbb{Z})$.

Then P corresponds to $\mu_1/N + \mu_2/N\,\tau_l$, and by choosing P suitably we can assume that $\mu_2 \in \{0, 1\}$ and $0 \leqslant \mu_1 < N-1$. The period q_l of $E \times K_{v_l}$ is defined as $q_l = e^{2\pi i \tau_l}$.

In order to compute $\delta_{v_l}(x)$ we have to manipulate formula (C_{19}) in [5], and we get for any point $Q = x_1 + x_2 \tau_l$ with $x_i \in \mathbb{R}$:

$$12\delta_{v_l}(Q) = (6x_2 - 6x_2^2 - 1) \log |q_l|_l - 12 \log \left| (1-t) \prod_{m=1}^{\infty} (1 - q^m t)(1 - q^m t^{-1}) \right|_l .$$

with $t = e^{2\pi i (x_1 + x_2 \tau_l)}$.

We use this expression in the special case: $Q = iP = i(\mu_1/N + (\mu_2/N) \cdot \tau_l)$: First assume that $\mu_2 = 0$ (i.e., x is "near" (∞) in K_{v_l}). We can take P to correspond to $1/N$, and so we get with $\zeta = e^{2\pi i/N}$:

$$12\delta_{v_l}(iP) = -\log |q_l|_l - 12 \log \left| (1-\zeta^i) \prod_{m=1}^{\infty} (1 - q_l^m \zeta^i)(1 - q_l^m \zeta^{-i}) \right|_l$$

or

$$\begin{aligned} 12\delta_{v_l}(x) &= -(N-1) \log |q_l|_l \\ &\quad - 12 \log \left| \prod_{i=1}^{N-1} (1-\zeta^i) \prod_{m=1}^{\infty} (1 - q_l^m \zeta^i)(1 - q_l^m \zeta^{-i}) \right|_l \\ &= -(N-1) \log |q_l|_l - 12 \log \left| N \frac{\prod (1 - q_l^{m \cdot N})^2}{\prod_{m=1}^{\infty} (1 - q_l^m)^2} \right|_l \end{aligned}$$

or

$$12\delta_{v_l}(x) = -\log \left| N^{12} \cdot \frac{\Delta(q_l^N)}{\Delta(q_l)} \right|_l . \tag{6}$$

Next we have to assume that $\mu_2 = 1$. We say: "x is near (0)." Let t_l be equal to $e^{2\pi i(\mu_1/N + (1/N)\tau_l)}$. Then we get:

$$\begin{aligned} 12\delta_{v_l}(x) &= \frac{N-1}{12N} \log |q_l|_l \\ &\quad -12 \log \left| \prod_{i=1}^{N-1} (1 - t_l^i) \prod_{m=1}^{\infty} (1 - q^m t_l^i)(1 - q^m t_l^{-i}) \right|_l \\ &= \frac{N-1}{12N} \log |q_l|_l - \log \left| \prod_{m=1}^{\infty} \left(\frac{1 - t_l^m}{1 - q_l^m} \right)^{24} \right|_l \end{aligned}$$

or

$$12\delta_{v}(x) = \log \left| \frac{\Delta(q_l)}{\Delta(t_l)} \right|_l . \tag{7}$$

Formulas (5), (6) and (7) together with (1) give:

$$\begin{aligned} &\sum_{\substack{v_l \in M_{K,\infty} \\ x \text{near}(\infty)}} \log \left| \frac{\Delta(q_l^N)}{\Delta(q_l)} \right|_l - \sum_{\substack{v_l \in M_{K,\infty} \\ x \text{near}(0)}} \log \left| \frac{\Delta(q_l)}{\Delta(t_l)} \right|_l \\ &= \sum_{\substack{\mathfrak{p} \in M_K' \\ v_{\mathfrak{p}}(j) < 0 \\ x \equiv (0) \bmod \mathfrak{p}}} \frac{N-1}{N} v_{\mathfrak{p}}(j) \log N(\mathfrak{p}) - \sum_{\substack{\mathfrak{p} \in M_K' \\ v_{\mathfrak{p}}(j) < 0 \\ x \equiv (\infty) \bmod \mathfrak{p}}} (N-1) v_{\mathfrak{p}}(j) \log N(\mathfrak{p}) + \varepsilon \end{aligned} \tag{8}$$

with $\varepsilon = c_N \cdot \log N$, $c_N \in \mathbb{Z}$ and $|c_N| \leqslant 48 |K : \mathbb{Q}|$.

2. Now let $^*K$ be again a nonstandard model of K and $N \in {}^*\mathbb{P}$ be a prime. Then our formulas can be interpreted in $^*K$ and remain valid if we replace M_K' by $^*M_K'$.

Assume that N is infinitely large. Then an immediate consequence of (6) is that if x is near to (∞) then

$$12\delta_{v_l}(x) \doteq -(N-1) \log |q_l|_l = \alpha_l \cdot 2\pi \operatorname{Im}(\tau_l)(N-1)) \tag{9}$$

with

$$\begin{aligned} \alpha_l &= 1, \quad && v_l \text{ real}, \\ &= 2, && v_l \text{ complex}. \end{aligned}$$

If x is near to (0) we have to be a little more careful. It can happen that some power t_l^m is infinitesimally close to 1, and so we have problems in computing $|\Delta(t_l)|$. But in this case $\mathrm{Im}(\tau_l)/N \approx 0$, and the worst case is that t_l is real and positive: We have to estimate $|\Delta(|t_l|)|_l$. But then

$$\Delta(e^{-2\pi \mathrm{Im}(\tau_l)/N}) = \left(\frac{\mathrm{Im}(\tau_l)}{N}\right)^{-12} \Delta(e^{-2\pi(N/\mathrm{Im}(\tau_l)}),$$

and hence:

$$\begin{aligned} 12\delta_{v_l}(x) &\doteq \frac{N-1}{N} \log |q_l|_l \\ &= -\frac{N-1}{N} \cdot \alpha_l \cdot 2\pi \,\mathrm{Im}(\tau_l) \qquad \text{if} \quad \mathrm{Im}(\tau_l) \not\ll N \end{aligned} \tag{10a}$$

or

$$12\delta_{v_l}(x) \leqslant \alpha_l \left(2\pi \frac{N}{\mathrm{Im}(\tau_l)} - 2\pi \,\mathrm{Im}(\tau_l) + 12 \log\left(\frac{N}{\mathrm{Im}(\tau_l)}\right)\right) \quad \text{if} \quad \mathrm{Im}(\tau_l) \ll N. \tag{10b}$$

Using (9), (10a) and (10b), we get from (8):

$$\begin{aligned} &\sum_{\substack{v_l \in M_{K,\infty} \\ x \,\mathrm{near}(\infty)}} \log |q_l|_l - \frac{1}{N} \sum_{\substack{v_l \in M_{K,\infty} \\ x \,\mathrm{near}(0)}} \log |q_l|_l \\ &\doteq \frac{1}{N} \sum_{\substack{\mathfrak{p} \in {}^*M_K' \\ v_{\mathfrak{p}}(j) < 0 \\ x \equiv (0) \bmod \mathfrak{p}}} v_{\mathfrak{p}}(j) \log N(\mathfrak{p}) - \sum_{\substack{\mathfrak{p} \in {}^*M_K' \\ v_{\mathfrak{p}}(j) < 0 \\ x \equiv (\infty) \bmod \mathfrak{p}}} v_{\mathfrak{p}}(j) \log N(\mathfrak{p}) \end{aligned} \tag{11}$$

and we can replace $\doteq$ by $\approx$ if $\mathrm{Im}(\tau_l) \gg 0$ for all l with x near (0) in K_{v_l}.

Now for $l = 1,\ldots, t$ we have $\log |j|_l \doteq -\log |q_l|_l$, and hence we can rewrite (11) in the following form:

$$\begin{aligned} &\frac{1}{N} \sum_{\substack{v_l \in M_{K,\infty} \\ x \,\mathrm{near}(0)}} \log |j|_l - \sum_{\substack{v_l \in M_{K,\infty} \\ x \,\mathrm{near}(\infty)}} \log |j|_l \\ &\doteq \frac{1}{N} \left(\sum_{\substack{\mathfrak{p} \in {}^*M_K' \\ v_{\mathfrak{p}}(j) < 0 \\ x \equiv (0) \bmod \mathfrak{p}}} v_{\mathfrak{p}}(j) \log N(\mathfrak{p}) \right) - \sum_{\substack{\mathfrak{p} \in {}^*M_K' \\ v_{\mathfrak{p}}(j) < 0 \\ x \equiv (\infty) \bmod \mathfrak{p}}} v_{\mathfrak{p}}(j) \log N(\mathfrak{p}). \end{aligned} \tag{11a}$$

4. Isogenies of Curves with Integral j-Invariants over Totally Real Fields

In this paragraph we assume that $^*K$ is a nonstandard model of a totally real number field K of degree m. Assume that E is an elliptic curve defined over $^*K$ with integral j-invariant j having a $^*K$-rational isogeny η of degree N ($N \in {}^*\mathbb{P}$). The corresponding point in $X_0(N)(^*K)$ is, usual, denoted by x.

If $v_1,\ldots, v_m$ are the archimedean internal places of $^*K$ then assume that x is near (0) in $^*K_{v_j} \cong {}^*\mathbb{R}$ for $j = 1,\ldots, k$, and that x is near (∞) in $^*K_{v_j}$ for $j = k+1,\ldots, m$.

η is defined over $^*K_{v_j} \equiv {}^*\mathbb{R}$, and this implies that the local periods q_j are reals; hence

$$\begin{aligned} \tau_j &= i \operatorname{Im}(\tau_j) && \text{if} \quad q_j > 0 \\ &= \tfrac{1}{2} + i \operatorname{Im}(\tau_j) && \text{if} \quad q_j < 0, \end{aligned}$$

and if x is near to (0) and $P = \mu_j/N + (1/N)\tau_j$ generates the kernel of η in K_{v_j} then

$$\begin{aligned} \mu_j &= 0 && \text{if} \quad q_j > 0 \\ &= \frac{N-1}{2} && \text{if} \quad q_j < 0 \end{aligned} \qquad \text{for} \quad 1 \leqslant j \leqslant k.$$

So (after changing the numeration if necessary) we can assume:

$$\begin{aligned} \mu_j &= 0 && \text{for} \quad 1 \leqslant j \leqslant l \\ \mu_j &= \frac{N-1}{2} && \text{for} \quad l+1 \leqslant j \leqslant k, \end{aligned}$$

and x near (∞) for $j = k+1,\ldots, m$.

Now it is possible to determine t_j: We have

$$\begin{aligned} t_j &= e^{(-2\pi \operatorname{Im}(\tau_j)/N)}, && j = 1,\ldots, l, \\ &= -e^{(-2\pi \operatorname{Im}(\tau_j)/N)}, && j = l+1,\ldots, k. \end{aligned}$$

If (for $1 \leqslant j \leqslant k$) $\operatorname{Im}(\tau_j)/N \not\approx 0$ then we get (formula (10a))

$$\log \frac{|\Delta(q_j)|_j}{|\Delta(t_j)|_j} \doteq \frac{2\pi \operatorname{Im}(\tau_j)}{N} - 2\pi \operatorname{Im}(\tau_j) = -\left(\frac{N-1}{N}\right) \cdot 2\pi \operatorname{Im}(\tau_j).$$

Now assume that $\operatorname{Im}(\tau_j)/N \approx 0$ and $1 \leqslant j \leqslant l$. Then we can restate (10b) in the form of an equality:

$$\log \left| \frac{\Delta(q_j)}{\Delta(t_j)} \right|_j \doteq 2\pi \frac{N}{\operatorname{Im}(\tau_j)} - 2\pi \operatorname{Im}(\tau_j) + 12 \log N - 12 \log \operatorname{Im}(\tau_j)$$

and we can replace $\doteq$ by $\approx$ if $\operatorname{Im}(\tau_j) \gg 0$.

The next case we have to look at is $l+1 \leqslant j \leqslant k$ and again $\operatorname{Im}(\tau_j)/N \approx 0$. Then

$$\Delta(t_j) = \left(2 \cdot \frac{\tau_j + (N-1)/2}{N} - 1\right)^{-12} \cdot \Delta(e^{2\pi i(1/2 + N/4 \operatorname{Im}(\tau_j))})$$

or

$$\log \left| \frac{\Delta(q_j)}{\Delta(t_j)} \right|_j \doteq -2\pi \operatorname{Im}(\tau_j) + \frac{\pi N}{2 \operatorname{Im}(\tau_j)} - 12 \log N + 12 \log(\operatorname{Im}(\tau_j)).$$

We put all the results of the computations made above in to formula (8), and we get:

$$\begin{aligned} &\sum_{\substack{j=1 \\ \operatorname{Im}(\tau_j)/N \not\approx 0}}^{k} 2\pi \operatorname{Im}(\tau_j) \left(\frac{1-N}{N}\right) \\ &\quad + \sum_{\substack{j=1 \\ \operatorname{Im}(\tau_j)/N \approx 0}}^{l} \left(2\pi \frac{N - \operatorname{Im}(\tau_j)^2}{\operatorname{Im}(\tau_j)} + 12 \log\left(\frac{\tau_j}{N}\right)\right) \\ &\quad + \sum_{\substack{j=l+1 \\ \operatorname{Im}(\tau_j)/N \approx 0}}^{k} \left(2\pi \frac{N - 4 \operatorname{Im}(\tau_j)^2}{4 \operatorname{Im}(\tau_j)} + 12 \log\left(\frac{\tau_j}{N}\right)\right) \\ &\quad + \sum_{j=k+1}^{m} 2\pi(N-1) \operatorname{Im}(\tau_j) \\ &\doteq c_N \cdot \log N, \end{aligned} \tag{12}$$

where $c_N \in \mathbb{Z}$ and $|c_N| \leqslant 48m$.

This formula imposes strong conditions on j. For example, assume that there is an isogeny, η'_N of E_N defined over $^*K$ with $\eta'_N \circ \eta_N \neq \pm N \cdot \mathrm{id}_E$. If $j \in \{1, \ldots, k\}$ and $\operatorname{Im}(\tau_j)/N \approx 0$ then

$$\tau_{N,j} = i \cdot \frac{N}{\operatorname{Im}(\tau_j)} \quad \text{or} \quad \tau_{N,j} = \frac{1}{2} + i \cdot \frac{N}{2 \operatorname{Im} \tau_j}.$$

Now if kernel $'(\eta'_N) = \langle P' \rangle$, and $P' = (1/N) \cdot \tau_{j,N}$ or $P' = (N-1)/2N + (1/N) \cdot \tau_{j,N}$, respectively, then we would get: $\eta'_N(E_N) = E$, and so E would be a curve with complex multiplication, and this implies: $j \in K$ (since there are only finitely many curves with complex multiplication defined over K).

So avoiding this special case we can use formula (12) for (E_N, η'_N) and get:

$$\sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N^2 \not\approx 0}}^{k} 2\pi \,\mathrm{Im}(\tau_j)\left(\frac{1-N}{N^2}\right)$$

$$+ \sum_{\substack{j=1 \\ 0 \not\approx \mathrm{Im}(\tau_j)/N \ll N}}^{l} \left\{2\pi \frac{N^2 - \mathrm{Im}(\tau_j)^2}{\mathrm{Im}(\tau_j)} + 12 \log\left(\frac{\mathrm{Im}(\tau_j)}{N^2}\right)\right\}$$

$$+ \sum_{\substack{j=l+1 \\ 0 \not\approx \mathrm{Im}(\tau_j)/N \ll N}}^{k} \left\{2\pi \left(\frac{N^2 - 4\,\mathrm{Im}(\tau_j)^2}{4\,\mathrm{Im}(\tau_j)}\right) + 12 \log \frac{\mathrm{Im}(\tau_j)}{N^2}\right\}$$

$$+ \sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N \approx 0}}^{l} 2\pi \frac{N(N-1)}{\mathrm{Im}(\tau_j)} + \sum_{\substack{j=l+1 \\ \mathrm{Im}(\tau_j)/N \approx 0}}^{k} 2\pi \left(\frac{(N-1)\cdot N}{4\,\mathrm{Im}(\tau_j)}\right)$$

$$+ \sum_{j=k+1}^{m} 2\pi N(N-1)\,\mathrm{Im}(\tau_j) \doteq c'_N \cdot \log N. \tag{12'}$$

Comparing (12) and (12') we get a contradiction if either $N \in {}^*\mathbb{P}\backslash\mathbb{P}$ or $j \in {}^*K\backslash K$ (for then at least at one place v_j we have $\mathrm{Im}(\tau_j) \gg 0$).

Hence we have proved the following.

PROPOSITION 4.1. *If N is a nonstandard prime or E is a nonstandard elliptic curve defined over $^*K$ with integral j-invariant then E has no $^*K$-rational cyclic isogeny of degree N^2.*

The standard version of this proposition is

COROLLARY 4.2. *Let K be a totally real number field. Then there are only finitely many elliptic curves with integral j-invariants (up to $\mathbb{C}$-isomorphisms) defined over K that have a cyclic K-rational isogeny whose degree is a square.*

The next step is to prove

PROPOSITION 4.3. *If E is defined over $^*K$ and has an integral j-invariant then E has only finitely many $^*K$-isogenies with cyclic kernels.*

Proof. Assume that there are infinitely many primes $N = N_0$, $N_1, \ldots, N_s, \ldots$, such that E has a $^*K$-rational isogeny of degree N_i.

If the numbers k_i and l_i are (with respect to N_i) analogously defined as k and l were with respect to N we can assume: For all i we have $k_i = k$ and $l_i = l$. Moreover we can assume that $\mathrm{Im}(\tau_j)/N \approx 0$ iff $\mathrm{Im}(\tau_j)/N_i \approx 0$ for all i.

Hence (12) (for N and N_i) gives:

$$\sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N \not\approx 0}}^{k} 2\pi \,\mathrm{Im}(\tau_j)\left(\frac{N_i - N}{N \cdot N_i}\right) + \sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N \approx 0}}^{l} 2\pi \frac{N - N_i}{\mathrm{Im}(\tau_j)} + \sum_{\substack{j=l+1 \\ \mathrm{Im}(\tau_j)/N \approx 0}}^{k} \frac{\pi(N - N_i)}{2\,\mathrm{Im}(\tau_j)} + \sum_{j=k+1}^{m} 2\pi(N - N_i)\,\mathrm{Im}(\tau_j) = c_N \log N - c_{N_i} \log N_i + \varepsilon_{N,N_i} \quad (13)$$

with $c_N, c_{N_i} \in \mathbb{Z}$, $|c_N| \leqslant 48 \cdot m$, $|c_{N_i}| \leqslant 48 \cdot m$, and

$$\varepsilon_{N,N_i} = \sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N \approx 0}}^{l} \log\left(\prod_{r=1}^{\infty} \frac{(1 - e^{-2\pi r(N/\tau_j)})^2}{(1 - e^{-2\pi r(N_i/\tau_j)})^2}\right) + \sum_{\substack{j=l+1 \\ \mathrm{Im}(\tau_j/N) \approx 0}}^{k} \log\left(\prod_{r=1}^{\infty} \frac{(1 - (1)^{r-1} e^{(-\pi r N/2\tau_j)})^2}{(1 - (-1)^{r-1} e^{(-\pi r N_i/2\tau_j)})^2}\right) + \varepsilon',$$

and ε' is finite.

There are only finitely many possibilities for c_{N_i}, and so we can assume that $c_N = c_{N_i}$.

Now multiply (13) by $1/2\pi(N_i - N)$. Then:

$$\sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N \not\approx 0}}^{k} \frac{\mathrm{Im}(\tau_j)}{N \cdot N_i} - \sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N \approx 0}}^{l} \frac{1}{\mathrm{Im}(\tau_j)} - \sum_{\substack{j=l+1 \\ \mathrm{Im}(\tau_j)/N \approx 0}}^{k} \frac{1}{4\,\mathrm{Im}(\tau_j)} - \sum_{j=k+1}^{m} \mathrm{Im}(\tau_j) = c_N \cdot \frac{\log(N/N_i)}{2\pi(N_i - N)} + \frac{\varepsilon_{N,N_i}}{2\pi(N_i - N)}. \quad (13a)$$

We use now $\eta_{N_i}(E)$ instead of E and the resulting equation compared with (13a) gives: $m = k$. Using Eq. (12) gives an estimation for

$$\sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N \not\approx 0}}^{k} \mathrm{Im}(\tau_j),$$

and this gives

$$\sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N \not\approx 0}}^{k} \frac{\mathrm{Im}(\tau_j)}{N}$$

is finite, and hence

$$\sum_{\substack{j=1 \\ \mathrm{Im}(\tau_j)/N \not\approx 0}}^{k} \frac{\mathrm{Im}(\tau_j)}{N \cdot N_i} \approx 0.$$

But this implies: $\mathrm{Im}(\tau_j) \gg 0$ for $j = 1,\ldots, m$. Hence we can assume (after replacing E by $\eta_{N_1}(E)$) if necessary that $\mathrm{Im}(\tau_j)/N_i \approx 0$ for infinitely many N_i and $j = 1,\ldots, m$, and this means that (13a) degenerates to

$$(N - N_i)\left(\sum_{j=1}^{l} \frac{1}{\mathrm{Im}\,\tau_j} + \sum_{j=l+1}^{m} \frac{1}{2\,\mathrm{Im}(\tau_j)}\right) = \frac{c_N}{2\pi} \log \frac{N}{N_i} + \varepsilon_{N,N_i} \qquad (13b)$$

and in the description of ε_{N,N_i} as given above we have: $\varepsilon' = 0$.

Again by applying a suitable isogeny we can assume that at least one τ_j has $\mathrm{Im}(\tau_j) \leqslant N^{1/2}$, and hence $x_i = N - N_i \ll N^{1/2}$. But for $0 < x \ll N^{1/2}$ one checks (for example, by using derivatives) that there are only finitely many intersections of the function

$$\varepsilon_{N,N-x} + c_N \log\left(1 + \frac{x}{N-x}\right) \quad \text{with } x\left(\sum_{j=1}^{l} \frac{1}{\mathrm{Im}\,\tau_j} + \sum_{j=l+1}^{m} \frac{1}{2\,\mathrm{Im}(\tau_j)}\right),$$

and so we finally get our contradiction, and the proposition is proved.

Remark. The proof of Proposition 4.3 shows that there is a bound that only depends on $[K:\mathbb{Q}]$ for the number of cyclic isogenies of E of prime degree rational over $^*K$.

Hence we get (with $\tau(d) = \#\{\text{divisor of } d \in \mathbb{N}\}$:

COROLLARY 4.4. *There is a number $M([K:\mathbb{Q}])$ such that for all elliptic curves with integral j-invariant and cyclic isogenies η of E that are K-rational we get: $\tau(|\ker(\eta)|) \leqslant M$.*

Now we look at the special case $K = \mathbb{Q}$. We have $m = 1$ and (with $\tau = \tau_1$): $\mathrm{Im}(\tau) \gg 0$ if E is not a standard curve.

We get from formula (12):

$$\frac{2\pi N}{\mathrm{Im}(\tau)} - 2\pi\,\mathrm{Im}(\tau) + 12\log(\mathrm{Im}(\tau)) - 12\log N \approx c_N \cdot \log N \quad (\text{if } q > 0) \qquad (14)$$

or

$$\frac{\pi N}{2\,\mathrm{Im}(\tau)} - 2\pi\,\mathrm{Im}(\tau) + 12\log(\mathrm{Im}(\tau)) - 12\log N \approx c_N \log N \quad (\text{if } q < 0). \qquad (15)$$

Let us look at (14). One sees at once $\mathrm{Im}(\tau) \approx N^{1/2}$, and if τ_N belongs to $\eta_N(E)$ then $\mathrm{Im}(\tau_N) \approx N^{1/2}$, too (since $\tau \cdot \tau_N = N$).

The function $f(X) = 2\pi X^2 - 12X\log X + X(12\log N - c_N \log N) - 2\pi N$ has a derivative $f'(X)$ whose value at the place $N^{1/2}$ is equal to

$4\pi N^{1/2} + 6 \log N - 12 + c_N \log N$, and this is an infinitely large number. Hence $f(X)$ cannot have two different zeros both infinitesimal near to $N^{1/2}$, and hence $\mathrm{Im}(\tau) = N^{1/2} = \mathrm{Im}(\tau_N)$. So we get: E has complex multiplication, but then E has to be a standard curve, and N a standard prime. In the same manner one shows that (15) implies $\mathrm{Im}(\tau) = N^{1/2}/2$, and again E has to be a standard curve.

Hence we proved

PROPOSITION 4.5. *There are only finitely many elliptic curves defined over $\mathbb{Q}$ (up to $\mathbb{C}$-isomorphisms) with integral j-invariant admitting a cyclic $\mathbb{Q}$-rational isogeny.*

Remarks. 1. If one looks at elliptic curves whose j-invariants are integral outside a given finite set S of places of $^*K$ one can get results similar to 4.1–4.4. (The bound then depends on the number of places in S.)

2. For $K = \mathbb{Q}$ we get Proposition 4.5 again by reduction theory of elliptic curves as developed in [2; 4, Section 5].

3. The condition that K is a totally real field was used in order to get a simple description of the kernels of the isogenies. It seems (and should be) possible to drop this condition. In the case of a quadratic imaginary field one gets an analogue of Proposition 4.5: The only curves with cyclic isogenies of arbitrary high degree with integral invariants are the curves with complex multiplication corresponding to fields with class number 1.

5. ISOGENIES OVER FIELDS SATISFYING AXIOM B

We assume in this section that K is a number field of degree m satisfying Axiom B. Let E be an elliptic curve defined over $^*K$ with a $^*K$-rational isogeny η of degree $N \in {}^*\mathbb{P} \backslash \mathbb{P}$ with corresponding point $x \in X_0(N)(^*K)$. We assume further that $j(E)$ is not an integer of $^*K$. Our aim is to prove that E has only finitely many cyclic $^*K$-rational isogenies.

We assume that $x \equiv (\infty) \bmod \mathfrak{p}$ for all $\mathfrak{p} \in {}^*M'_K$ with $v_\mathfrak{p}(j) < 0$. (It is a consequence of Axiom B that either η_N or $w(\eta_N)$ satisfies this assumption.)

For the infinite places we use the same notations as in Section 4, and we get

$$\frac{2\pi}{N} \sum_{j=1}^{k} \alpha_j \,\mathrm{Im}(\tau_j) = 2\pi \sum_{j=k+1}^{t} \alpha_j \,\mathrm{Im}(\tau_j) + \sum_{\substack{\mathfrak{p} \in {}^*M'_K \\ v_\mathfrak{p}(j) < 0}} (-v_\mathfrak{p}(j)) \log N(\mathfrak{p}) + \delta_N \qquad (16)$$

with

$$|\delta_N| \leqslant \sum_{j=1}^{k} \alpha_j \frac{\pi}{6 \operatorname{Im} \tau_j}.$$

We assume that $N_1 \in {}^*\mathbb{P}$ has the same properties as N, but $N_1 \neq N$. There is an ${}^*K$-rational isogeny $\eta_{N_1}: E \to E_{N_1}$ and if x_1 corresponds to η_{N_1} then $x_1 \equiv (\infty) \bmod \mathfrak{p}$ for $v_{\mathfrak{p}}(j) < 0$, and x_1 near (∞) in K_{v_j} for $j = k+1, \ldots, t$.

If E has infinitely many cyclic ${}^*K$-isogenies then Axiom B implies that there are infinitely many N_1 satisfying these conditions if we choose N appropriately.

The curve E_{N_1} has an induced isogeny η'_N of degree N, and this isogeny gives us the formula

$$\frac{2\pi}{N}\left(\sum_{j=1}^{k} \alpha_j \operatorname{Im}(\tau_j^1)\right) \doteq N_1 \cdot \left(2\pi \sum_{j=k+1}^{t} \alpha_j \operatorname{Im}(\tau_j) + \sum_{\substack{\mathfrak{p} \in {}^*M_K' \\ v_{\mathfrak{p}}(j) < 0}} (-v_{\mathfrak{p}}(j) \log N(\mathfrak{p})\right) \tag{16'}$$

(here τ_j^1 corresponds to E_1 in K_{v_j}).

Now assume that $\operatorname{Im}(\tau_j^1) \geqslant N_1 \operatorname{Im}(\tau_j)$ for $j \in \{1, \ldots, k\}$. Then: $\tau_j = (\tau_j^1 + h)/N_1$ with some h, and so $\operatorname{Im}(\tau_j^1) = N_1 \cdot \operatorname{Im}(\tau_j)$, and this would imply that x_1 is near (∞) in K_{v_j}. We know even more: Since $(2\pi/N)$ $(\sum_{j=1}^{k} \alpha_j \operatorname{Im}(\tau_j)) \gg 0$ we have a j with $\operatorname{Im}(\tau_j)/N \gg 0$. Hence we have for this j: $\operatorname{Im}(\tau_j^1) \doteq \operatorname{Im}(\tau_j)/N_1$ if $N_1 < N$, and so

$$\frac{-N_1 \cdot \operatorname{Im}(\tau_j) + \operatorname{Im}(\tau_j^1)}{N \cdot N_1} \doteq \frac{-1}{N} \operatorname{Im}(\tau_j) + \frac{\operatorname{Im}(\tau_j)}{N_1^2 \cdot N} \ll 0,$$

and hence (16') leads us to a contradiction.

So we proved:

PROPOSITION 5.1. *If K is a number field satisfying Axiom* B *then there is a bound $M(K)$ such that any elliptic curve with nonintegral j-invariant has at most $M(K)$ K-rational cyclic isogenies. (If K is totally real this is true for all j-invariants.)*

To end we assume that K is equal to $\mathbb{Q}$. (If K is a quadratic imaginary field then some of the results can be proved in this case too; cf. [2].) In this case formula (16) gives:

$$\frac{2\pi}{N} \operatorname{Im}(\tau) = \sum_{\substack{\mathfrak{p} \in {}^*M_{\mathbb{Q}}' \\ v_{\mathfrak{p}}(j) < 0}} -v_{\mathfrak{p}}(j) \log N(\mathfrak{p}) + \delta_N \tag{17}$$

with $\delta_N \approx \pi/6 \operatorname{Im}(\tau)$.

We assume: $N \in {}^*\mathbb{P}\backslash\mathbb{P}$, so $j \notin \mathbb{Q}$, and hence we have either $\mathrm{Im}(\tau) \gg 0$ or there is a $\mathfrak{p} \in {}^*M'_{\mathbb{Q}}$ with $-v_{\mathfrak{p}}(j) \log N(\mathfrak{p}) \gg 0$.

In the latter case (17) implies again that $\mathrm{Im}(\tau) \gg 0$. So $\delta_N \approx 0$, and we have:

$$\frac{2\pi}{N}\mathrm{Im}(\tau) \approx \sum_{\substack{\mathfrak{p} \in {}^*M'_K \\ v_{\mathfrak{p}}(j) < 0}} -v_{\mathfrak{p}}(j) \log N(\mathfrak{p}) \qquad \text{and} \qquad \mathrm{Im}(\tau) \gg N,$$

hence $\mathrm{Im}(\tau_N) \gg 0$, where τ_N belongs to $\eta_N(E)$ in ${}^*\mathbb{R}$.

At first assume that the denominator of j is bounded. Then E has potentially good reduction in all primes p that are larger than a finite number p_0. In particular, E has potentially good reduction in N, and using the results of [4], just as described in [2], concerning the Galois representation of $G({}^*\bar{\mathbb{Q}}|{}^*\mathbb{Q})$ given by the action on the points of order N, we get a contradiction: There is a standard prime P such that E has potentially good reduction mod p, and in the trace formula in Corollary 6.1 of [2] for the Frobenius with respect to p we get equalities (as $N \gg 0$) that contradict the Riemann hypotheses for elliptic curves defined over finite fields.

Remark. We could say more about the reduction type of E. Assume $q > 0$. If τ_N is finite then we get from (8) and (12):

$$2\pi \frac{N - \mathrm{Im}(\tau_N)^2}{\mathrm{Im}(\tau_N)} + 12 \log \frac{\tau_N}{N} \approx c_N \cdot \log N - (N-1) \sum_{\substack{\mathfrak{p} \in {}^*M'_{\mathbb{Q}} \\ v_{\mathfrak{p}}(j) < 0}} v_{\mathfrak{p}}(j) \log N(\mathfrak{p}),$$

or

$$\frac{2\pi N}{N-1} \approx -\mathrm{Im}(\tau_N) \cdot \sum_{\substack{\mathfrak{p} \in {}^*M'_{\mathbb{Q}} \\ v_{\mathfrak{p}}(j) < 0}} v_{\mathfrak{p}}(j) \log N(\mathfrak{p}).$$

As $\mathrm{Im}(\tau_N) \geqslant 1$ we get:

$$\sum_{\substack{\mathfrak{p} \in {}^*M'_{\mathbb{Q}} \\ v_{\mathfrak{p}}(j) < 0}} -v_{\mathfrak{p}}(j) \log N(\mathfrak{p}) \leqslant 2\pi.$$

A similar computation shows that, if $q < 0$, we get also:

$$-\sum_{\substack{\mathfrak{p} \in {}^*M'_{\mathbb{Q}} \\ v_{\mathfrak{p}}(j) < 0}} v_{\mathfrak{p}}(j) N(\mathfrak{p}) \leqslant 2\pi.$$

So we get: If E has a ${}^*\mathbb{Q}$-rational isogeny of degree N ($N \in {}^*\mathbb{P}\backslash\mathbb{P}$) and the j-invariant has a bounded denominator then this denominator is at most equal to 6.

This result is for j-invariants with bounded denominator an analogue of Corollary 4.4 in [2].

Now assume that $\mathrm{Im}(\tau_N)/N \neq 0$. Then $(E_N, w(\eta_N))$ is infinitely near to (∞). In order to prove that $(E_N, w(\eta_N))$ cannot exist we have to use the description of the behaviour of the mapping $f: X^0(N)/{}^*\mathbb{Z} \to \bar{J}/{}^*\mathbb{Z}$ near (∞), given in [2]: Near (∞) f is given by a power series $\sum_{i=1}^{\infty} a_i q^i$, a_1 is finite (it can happen that $2|a_1$, but $v_2(a_1)$ has to be finite), and the a_i's are not growing too fast: They can be defined inductively by using eigenvalues of Hecke operators. Mazur used this description to prove that f is formally unramified in primes other than 2 in (∞), we use this to show that a point lying infinitely near to (∞) in $X_0(N)({}^*\mathbb{C})$ is not mapped into $f((0))$. Hence $f(x_N) \neq f((0))$. But as $x_N \equiv (0) \bmod \mathfrak{p}$ for a $\mathfrak{p} \in {}^*M'_{\mathbb{Q}}$ with $v_{\mathfrak{p}}(j) < 0$ we must have: $f(x_N) = f((0))$, and hence we have obtained a contradiction.

So we proved the following:

PROPOSITION 5.2. *There is no elliptic curve defined over* ${}^*\mathbb{Q}$ *having a* ${}^*\mathbb{Q}$*-rational isogeny with cyclic kernel of degree* $N \gg 0$.

The standard version of this proposition gives us a qualitative equivalent of the result of Mazur in [2], where he determines all isogenies of prime degree being rational over $\mathbb{Q}$.

COROLLARY 5.3. *There is an* $M \in \mathbb{N}$ *with the following property: If* E *is an elliptic curve defined over* $\mathbb{Q}$ *with a cyclic* $\mathbb{Q}$*-rational isogeny of degree larger than* M *then the denominator of the* j*-invariant of* E *is bounded by* 6, *and hence there are only finitely many elliptic curves (up to* $\mathbb{C}$*-isomorphisms) having a* $\mathbb{Q}$*-rational isogeny of prime degree greater than* 7.

REFERENCES

1. B. MAZUR, Modular curves and the Eisenstein ideal, *Inst. Hartes Études Sci. Publ. Math.* **47** (1977).
2. B. MAZUR, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.
3. A. ROBINSON AND P. ROQUETTE, On the finiteness theorem of Siegel and Mahler concerning diophantine equations, *J. Number Theory* **7** (1975), 121–176.
4. J. P. SERRE, Proprietes galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
5. H. G. ZIMMER, Quasifunctions on elliptic curves over local fields, *J. reine u. angew. Math.* **307/308** (1979), 221–246.